IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In re Search Warrant No. 16-1061-M to Google	:	**Misc. No. 16-1061-M**
	:	**FILED UNDER SEAL**

UNITED STATES' REPLY TO GOOGLE'S RESPONSE

On August 19, 2016, this Court issued a search warrant, pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A), commanding Google to disclose to the government the contents of three separate Google accounts. This criminal grand jury investigation involves a wire fraud scheme committed in the United States, by a United States citizen who was residing in the United States. The victim is a United States corporation, doing business in the United States, headquartered on the East Coast. During the time period relevant to this investigation, the target worked for this corporation in the Eastern District of Pennsylvania. The target allegedly stole large amounts of highly valuable corporate information by uploading the data from his work computer to his Google account. The search warrant's affidavit provided probable cause to believe that the target's Google account contains evidence of his crimes. In short, the crimes under investigation occurred in the United States, were committed by a United States citizen against a United States victim – and those crimes were facilitated by using his Google account, including its related e-mail and Google Drive services.

Google only partially complied with the search warrant, refusing to produce all of the information in its possession, custody, and control that is subject to the warrant. Google instead limited its production to records that it said it could determine were stored within the United States.

The government then moved to enforce the warrant, and the Court ordered Google to file a response. Google has done so and raises two issues. First, without stating with certainty whether

it has produced all of the responsive data that was stored in the United States, Google asserts that it does not have to produce data that is or might be stored outside of the country. (*See* Google's Response to November 22, 2016 Order to Show Cause and Motion to Amend Non-Disclosure Order ("Google's Response") at 2 ("On September 7, 2016, and in a supplemental production on October 11, Google produced responsive records that were confirmed to be stored in the United States and, pursuant to the *Microsoft* decision, did not produce records that were not.) and at 5 ("The warrant also cannot reach records if it is unknown whether the records are located in the United States").[1] Google argues that the Second Circuit's decision in *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) (hereafter "*Microsoft*" or "the *Microsoft* decision") precludes it from producing any data that is or might be held in a foreign server.

Second, admitting that it has no knowledge of the facts justifying the Court's non-disclosure order, Google argues that the Court's order protecting the compelling government interest in the ongoing criminal investigation cannot overcome Google's interests in publicly disclosing the nature of the government's investigation.

The government suggests that Google is wrong, for a variety of reasons, all of them compelling. With respect to Google's first issue – the primary issue in this litigation – both the Stored Communications Act and Third Circuit precedent hold that a party subject to this Court's

[1] To support this assertion, Google cites *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). In that case, the government sought a search warrant – under Rule 41 of the Federal Rules of Criminal Procedure and not under the Stored Communications Act – to conduct a remote search of a computer in the district because it could not determine the location of the computer used to commit the crime. The court held that it had no authority to issue such a warrant. The case has since been overruled by the 2016 amendments to Rule 41 of the Federal Rules of Criminal Procedure. In that case, the government made its best efforts to locate the offending computer before seeking the warrant in the only logical district it could apply. That is a far cry from this case in which Google either will not determine the location of data that it holds, or cannot because of a storage system that it has created.

jurisdiction can be compelled to disclose materials in its custody, even if that material is stored elsewhere – a conclusion supported by the weight of Congressional intent. Further – and the government says this with the utmost respect for our sister circuits – the *Microsoft* decision is incorrect, inconsistent with the weight of authority, not binding on this court, and should not be followed. Critically, applying the *Microsoft* decision to the present case would lead to patently absurd results – including the fact that the government could *never* access *any* of Google's data stored abroad. In this case, that data consists of Google e-mails and attachments, sent by U.S. citizens, located in the United States, to recipient U.S. citizens, also located in the United States, which facilitated crimes that occurred in the United States against victims located in the United States. The government hereby responds to Google's arguments in this filing.

I. THE STORED COMMUNICATIONS ACT AND PRECEDENT OF THIS CIRCUIT HOLD THAT A PARTY SUBJECT TO THE COURT'S JURISDICTION CAN BE COMPELLED TO DISCLOSE MATERIALS IN ITS CUSTODY.

A. The Stored Communications Act Authorizes Disclosure of Information When A "Court of Competent Jurisdiction" Has Issued a Warrant to Search Such Information.

The Stored Communications Act provides the authority for this Court to issue a warrant (1) requiring Google to disclose particular information, and (2) authorizing the government to search the disclosed information as set forth in the attachments to the warrant. *See* 18 U.S.C. § 2703(a)-(c) (requiring the disclosure of information by providers of electronic communication service and remote computing service when warrants authorize the search of such information). Such warrants are appropriately issued "by a court of competent jurisdiction." 18 U.S.C.

§ 2703(a)-(c). That includes this Court because it has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(i).

B. The Scope of a Warrant Under the Stored Communications Act Is Not Limited to Information Geographically Located in the District.

Rule 41(b) of the Federal Rules of Criminal Procedure generally requires that the property to be searched for and seized "be located in the district." (Compare Rule 41(b)(1) with 41(b)(2)-(6)). The Stored Communications Act, however, operates differently: it explicitly broadens the jurisdiction of courts to issue warrants for property located outside the district. In addition to creating jurisdiction when the information is stored in the same district, the Act also defines a "court of competent jurisdiction" as a court having jurisdiction over the offense under investigation or a court in the district in which the provider is located. *See* 18 U.S.C. §§ 2703(a)-(c) and 2711(3).[2]

Accordingly, under the broader jurisdiction granted by the Stored Communications Act, the information required to be disclosed pursuant to a warrant need not be in this district at the time the warrant is issued. Fed. R. Crim. P. 41(a)(1) explicitly recognizes such statutory provisions.

---

[2] The full definition of "court of competent jurisdiction" includes –

> (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that –
>
> (i) has jurisdiction over the offense being investigated;
> (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or
> (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or
>
> (B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants[.]

18 U.S.C. § 2711(3).

("This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances."). Accordingly, the Stored Communications Act recognizes that, in the context of certain electronic information (such as the content of e-mails held and controlled by providers of electronic communications service and computing service), the fact that such information is electronically stored in remote locations does not limit the ability of this Court to require it to be gathered and produced in this district. In that regard, the Stored Communications Act implements the fundamental principle, detailed below, that requiring the production in a given district of information located abroad does not trigger extraterritorial issues because the act of compulsion takes place domestically.

C. Requiring Google to Gather and Disclose Information Within the United States Is a Domestic Application of the Stored Communications Act, Even When Google Must Gather Information Stored Abroad.

Requiring Google to take steps in the United States to gather the requested information, even if stored abroad, and to disclose that information to the government in the United States, is a domestic application of the Stored Communications Act. The geographic location of the information to be gathered does not change that.

This is not a novel concept. On the contrary, it is well-settled in this Circuit, and others, that the power to require a person to disclose information applies to all information in that person's custody or control, regardless of where the information is located. *Hay Group, Inc. v. E.B.S. Acquisition Corp.*, 360 F.3d 404, 412 (3d Cir. 2004) (Alito, J.) ("'Production' refers to the delivery of documents, not their retrieval, and therefore 'the district in which the production . . . is to be made' is not the district in which the documents are housed but the district in which the subpoenaed party is required to turn them over."); *Gerling Int'l Ins. Co. v. CIR*, 839 F.2d 131, 140 (3d Cir. 1988) (explaining that, under the rule governing the production of documents and other evidence

in tax court, "[t]he location of the documents, whether within the territorial jurisdiction of the court or not, is irrelevant").[3]

These cases reason that because a court's ability to require disclosure is premised on the court's jurisdiction over the person, the compulsion is domestic. This conclusion remains the same, even when some of the information required to be disclosed must be gathered from outside the United States. *See* Restatement (Third) of Foreign Relations Law § 442(1)(a) (1987) (making clear that "[a] court or agency in the United States, when authorized by statute or rule of court, may

---

[3] The Third Circuit is not alone in this regard. *See, e.g., Reinsurance Co. of Am. v. Administratia Asigurarilor de State (Admin. of State Ins.)*, 902 F.2d 1275, 1281 (7th Cir. 1990) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information . . . is outside the United States."); *United States v. Bank of Nova Scotia*, 691 F.2d 1384, 1389-90 (11th Cir. 1982) (affirming the district court's order enforcing a grand jury subpoena against a Bahamian bank which was "subpoenaed while subject to the jurisdiction of [the district court]," where the subpoena required disclosure of records located in the Bahamas); *Marc Rich & Co. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983) (a witness may not "resist the production of [subpoenaed] documents on the ground that the documents are located abroad ... [t]he test for production of documents is control, not location") (citations omitted); *In re Anschuetz & Co., GmbH*, 754 F.2d 602, 614 n.29 (5th Cir. 1985) (noting that "[i]t is not ipso facto a defense to a discovery request that the law of a foreign country may prohibit production or disclosure"); *United States v. Vetco Inc.*, 691 F.2d 1281, 1288-91 (9th Cir. 1981) (affirming the district court's exercise of its jurisdiction to enforce a summons requiring a Swiss subsidiary of an American firm to produce documents that were all held in Switzerland, even though the firms' compliance would require it to violate Swiss law); *In re Sealed Case*, 832 F.2d 1268, 1284 (D.C. Cir. 1987), *abrogated on other grounds by Braswell v. United States*, 487 U.S. 99 (1988) (holding that a subpoena for documents in Switzerland is enforceable by the district court if it has personal jurisdiction over the companies whose records are sought); *see also In re Grand Jury 81-2*, 550 F. Supp. 24, 26-30 (W.D. Mich. 1982) (granting a motion to compel the production of records in the possession of a German bank through grand jury subpoenas – even though the records sought were located in Germany and the bank was neither a target of the grand jury investigation nor a party to the proceedings before the grand jury – where the bank was maintaining an active branch office in New York and had deliberately and continually operated within the jurisdiction of the United States); *cf. Quaak v. Klynveld Peat Marwick Goerdeler Bedrijfsrevisoren*, 361 F.3d 11, 16 (1st Cir. 2004) (affirming order requiring defendant auditing firm to produce documents in discovery it maintained overseas); *Cent. Wesleyan Coll. v. W.R. Grace & Co.*, 143 F.R.D. 628, 643-47 (D.S.C. 1992), aff'd, 6 F.3d 177 (4th Cir. 1993) (granting plaintiff's motion to compel the production of documents located in Canada); *Lyons v. Bell Asbestos Mines*, Ltd., 119 F.R.D. 384, 389 (D.S.C. 1988) ("Unquestionably, this court possesses the power to enter an order under Rule 37(a) compelling defendant Asten-Hill to respond to interrogatories or to produce documents located abroad."); *Skky, Inc. v. Thumbplay Ringtones, LLC*, 2014 WL 11429038, at *3-*6 (D. Minn. Apr. 4, 2014) (granting plaintiff's motion to compel defendants to produce documents located in Québec).

order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States"). Courts have long been empowered to exert authority on people and entities over whom they have jurisdiction, even if that authority has consequences overseas. *See, e.g., Blackmer v. United States*, 284 U.S. 421, 438 (1931) ("The jurisdiction of the United States over its absent citizen, so far as the binding effect of its legislation is concerned, is a jurisdiction in personam, as he is personally bound to take notice of the laws that are applicable to him and to obey them."); *Hale v. Henkel*, 201 U.S. 43, 75 (1906) ("It would be a strange anomaly to hold that a state, having chartered a corporation to make use of certain franchises, could not, in the exercise of its sovereignty, inquire how these franchises had been employed, and whether they had been abused, and demand the production of the corporate books and papers for that purpose.").

This fundamental concept – that a court's power to compel disclosure is directed to the person (*in personam*), not the items to be produced (*in rem*) – was well-established at common law long before Congress enacted Section 2703 of the Stored Communications Act in 1986. It was not, therefore, a radical change when, in 2001, Congress broadened the jurisdiction of courts to issue warrants for information located outside the normal jurisdiction of the issuing court. Accordingly, the decision not to impose a Rule 41-type territorial limitation on warrants issued pursuant to the Stored Communication Act, but rather to define a "court of competent jurisdiction" to include *any* Federal court that has jurisdiction over the offense being investigated, must be read as a deliberate choice by Congress to authorize a court to require the disclosure of information not located in the district. "'[W]hen a statute covers an issue previously governed by the common law,' [courts] must presume that 'Congress intended to retain the substance of the common law.'" *Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351, 1363 (2013) (quoting *Samantar v. Yousuf*,

560 U.S. 305, 320 n.13 (2010)). Indeed, in light of the settled common law on the *in personam* nature of a court's power to compel the disclosure of documents, as well as Section 2703's focus on regulating such disclosure, there can be little doubt that Congress envisioned "a court of competent jurisdiction" as one empowered to compel a U.S.-based provider of electronic communications service or remote computer service to disclose information in its custody and control – regardless of where that information may be when the provider takes action in the United States to gather it.

D. Congress Has Since Taken Unequivocal Action Confirming That It Believes the Stored Communications Act Requires Disclosure of Information, Even If Stored Abroad.

Action taken by Congress since it enacted the Stored Communications Act further confirms that Congress intended to require providers in the U.S. to disclose information stored elsewhere to U.S. authorities. In 2006, the Senate ratified the Council of Europe Convention on Cybercrime (the "Cybercrime Treaty" or "Treaty"), the leading international treaty concerning combatting cybercrime and the collection of electronic evidence. Article 18 of the Cybercrime Treaty requires its signatories to "adopt such legislative and other measures as may be necessary to empower its competent authorities to order . . . a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium[.]" Cybercrime Treaty, Art. 18.1.a.[4]

[4] In ratifying the Cybercrime Treaty, the United States Senate was asked to provide advice and consent on a multilateral treaty outlining, *inter alia*, requirements for its signatories "to have the ability to investigate computer-related crime effectively and to obtain electronic evidence in all types of criminal investigations and proceedings." *See Letter of Transmittal to Senate from the President* ("Letter of Transmittal") at III, Treaty Doc. 108-11. The signed treaty was submitted to the Senate by then-president George W. Bush accompanied by a letter of submittal from the Department of State, signed by Colin L. Powell, along with its "official Explanatory Report, which was also adopted by the [Council of Europe's] Committee of Ministers on November 8, 2001." *See Letter of Submittal to Senate from the Department of State* ("Letter of Submittal") at V, Treaty Doc. 108-11.

The Department of State's interpretation of Article 18, as presented to Congress, was that under subsection (a), a "person" includes a "third party custodian of data, such as an ISP." *See Letter of Submittal* at XV ("Under Article 18 authorities must be able to order a person, *including third party custodian of data, such as an ISP* [meaning "internet service provider"], to produce data, including subscriber information, that is in that person's possession or control.") (emphasis added); *see also Abbott v. Abbott*, 560 U.S. 1, 15 (2010) (referring to the "well established canon of deference" to the "Executive Branch's interpretation of a treaty") (relying on *Sumitomo Shoji America, Inc. v. Avagliano*, 457 U.S. 176, 185 (1982)). Significantly, this provision focuses its territorial limit, "in [the compelling authority's] territory," on the location of the person being ordered, not on the location of the system or storage medium. Further, the official Explanatory Report transmitted to the Senate noted that the use of the term "possession or control" as used in paragraph 1(a) of Article 18 of the Cybercrime Treaty "refers to physical possession of the data concerned in the ordering Party's territory, *and situations* in which the data to be produced *is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory . . . .*" *See* Explanatory Report ¶ 173 (emphasis added); *see also* Letter of Submittal at V (specifically referencing the "official Explanatory Report" for review by the Senate). Simply stated, all of the signatories to the Cybercrime Treaty – including the United States – view the production of data stored abroad, but controllable and accessible from within the signatories' borders, as a domestic act, and require that legislation exist to ensure each signatory has such power.

When it ratified the Treaty, the Senate agreed with the President, the Department of State, and the Department of Justice that federal statutes governing the collection of electronic data – i.e., the Stored Communications Act – already provided the power required under Article 18. *See* Letter

of Transmittal at III (with certain reservations and declarations not including Article 18, the Cybercrime Treaty "would not require implementing legislation for the United States"); Letter of Submittal at VI ("The [Cybercrime Treaty] would not require implementing legislation for the United States."); S. Hrg. 108-721 at 9 (testimony of Samuel M. Witten, Deputy Legal Advisor, U.S. Department of State, before the Senate Committee on Foreign Relations that "[t]he [Cybercrime Treaty] would not require implementing legislation for the United States") *and* 27 (testimony of Bruce Swartz, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, that "the [Cybercrime Treaty] will be implemented in the United States under our existing statutes"). The Senate Committee on Foreign Relations report specifically notes that Articles 16 through 21 of the Treaty require parties to have the ability to "preserve, search, and seize stored computer data" and conclude that "[i]t bears emphasis that all of these investigative tools *are already provided for under U.S. domestic law*." *Senate Executive Report* 109-6 (emphasis added).

The Cybercrime Treaty was ratified in 2006, which was well after not only the original enactment of the Stored Communications Act in 1986, but also its substantial modification in 2001, when Congress deliberately broadened the jurisdiction of courts to issue warrants so that it includes information outside the jurisdiction of the issuing court (as discussed above). Congress plainly saw no need to amend the Act or create new legislation to meet the Treaty obligations described above. Moreover, Congress has since revisited the Stored Communications Act to amend it in related ways, but still has not concluded it was necessary to add any new language or provisions to empower courts to compel the disclosure of foreign-stored data from domestic providers as required by Article 18. *See* 123 Stat. 2086 (enacting the Foreign Evidence Request Efficiency Act

of 2009, which made certain amendments to the Stored Communications Act designed to address requests by foreign law enforcement with respect to foreign criminal investigations).

Accordingly, there now have been two occasions – first when the Senate ratified the Cybercrime Treaty, and then when Congress enacted subsequent amendments to the Stored Communications Act – on which Congress has acted in a manner consistent with its view that the Stored Communications Act gives courts the power to require U.S. service providers to disclose information, pursuant to a warrant, in their possession or control, regardless of from where the data must be gathered. This is further and powerful indication that the Stored Communications Act must be read to authorize the production of information domestically, even if stored remotely abroad. Where Congress interprets a prior enactment in the context of the "proceed[ing] formally through the legislative process," that interpretation is entitled to "great weight in statutory construction." *Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc.*, 477 U.S. 102, 118 n.13 (1980) (explaining *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367, 380–81 (1969)); *Commodity Futures Trading Comm'n v. Schor*, 478 U.S. 833, 846 (1986) ("It is well established that when Congress revisits a statute giving rise to a longstanding administrative interpretation without pertinent change, the 'congressional failure to revise or repeal the agency's interpretation is persuasive evidence that the interpretation is the one intended by Congress.") (quoting *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 274-75 (1974)); *see also Bell v. New Jersey*, 461 U.S. 773, 784-85 (1983) ("Of course, the view of a later Congress does not establish definitively the meaning of an earlier enactment, but it does have persuasive value.").

E. The Microsoft Decision Is Incorrect, Inconsistent with The Weight of Authority, Does Not Bind This Court, and Should Not Be Followed.

In *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016), the Second Circuit overruled a magistrate judge and a district judge, each of whom had found that the Stored

Communications Act required Microsoft to disclose information in its custody, even if it had to require an employee in the United States to retrieve information from computers outside the United States in order to disclose it in New York. *Id.* at 222. In rejecting the long-standing and previously unquestioned scope of the Stored Communications Act, the Second Circuit held, for the very first time, "that [a] [Stored Communications Act] warrant may reach only data stored within United States boundaries." *Id.* at 221.[5]

The Second Circuit's reasoning is seriously flawed and should be rejected in this Circuit for at least three reasons. First, it is inconsistent with the well-established rule that a court, once it has jurisdiction over a person, can compel that person to disclose information regardless of from where the person must gather such information. *Hay Group*, 360 F.3d at 412; *see* pp 4-6, above.

Second, the Second Circuit erroneously concluded that because the Stored Communications Act uses the term "warrant," Congress implicitly imported the "traditional[] . . . territorial limitations" that apply to warrants such as those imposed by Federal Rule of Criminal Procedure 41(b). *Microsoft*, 829 F.3d at 201. But that conclusion ignores explicit language in the Stored Communications Act reflecting Congress' intent *not* to impose such limitations, as well as Congress' view that no additional legislation is needed to comply with the obligations of the Cybercrime Treaty. That conclusion also ignores the fact that the use of the term "warrant" is more logically understood *not* as a geographic limitation inconsistent with the plain language of the Stored Communications Act (see discussion above), but as a description of the procedures to be followed in order to require the information to be produced – exactly as the plain language repeatedly indicates. *See* 18 U.S.C. § 2703(a) ("pursuant to a warrant using the procedures

[5] On October 13, 2016, the United States moved for rehearing and rehearing *en banc* of that decision. *See* General Docket, Court of Appeals for the Second Circuit, Case No. 14-2985, Docket Data Entry # 316.

described in the Federal Rules of Criminal Procedure"); § 2703(b)(1)(A) (same); § 2703(c)(1)(A) (same). Indeed, as the concurring opinion in *Microsoft* notes, the "the SCA does not describe the warrant" as a Rule 41 search warrant; instead, "it simply authorizes the government to *require the service provider to disclose* certain communications to which it has access." *Microsoft*, 829 F.3d at 226-28 (Lynch, J., concurring) (emphasis in original).

Third, the Second Circuit misapplied the Supreme Court's two-step framework for analyzing extraterritoriality as explained in *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247 (2010), *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659 (2013), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2100-01 (2016). "When a statute gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255. Accordingly, "[a]t the first step, [a court must] ask whether the presumption of extraterritoriality has been rebutted – that is whether the statute gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco,* 136 S. Ct. at 2101. At the second step, triggered only if a provision is found not to apply extraterritorially, courts must determine whether the case nonetheless "involves a domestic application of the statute . . . by looking to the statute's 'focus.'" *Id.* Ultimately, if the relevant conduct "occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad." *Id.* (emphasis added).

The *Microsoft* court correctly concluded that the presumption against extraterritoriality applies to the Stored Communications Act. *Microsoft*, 829 F.3d at 216. It erred, however, at the second step of *Morrison* when it determined that (1) the relevant "focus" of Section 2703 of the Stored Communications Act under a *Morrison* analysis is privacy, as opposed to disclosure, and (2) any invasion of that privacy "takes place . . . where the customer's protected content is accessed – here, where it is seized by Microsoft, acting as an agent of the government." *Id.* at 216-20.

In discerning the focus, the *Microsoft* court concluded that Section 2703's warrant provision evokes a focus on privacy because "Rule 41 is undergirded by the Constitution's protections of citizens' privacy[.]" Microsoft, 829 F.3d at 217 (quotations omitted). The court then looked to other aspects of the Stored Communications Act, noting that various provisions included mechanisms designed to protect individuals' "privacy interest in their stored communications." *Id.* at 217-18. Finally, the court cited legislative history indicating that Congress sought to "ensure protections traditionally afforded by the Fourth Amendment" and "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." *Id.* 219-20 (quotations omitted).

The Second Circuit erred, however, when it went beyond Section 2703 to look at the Stored Communications Act as a whole in order to discern its "focus," because step two of a proper extraterritoriality analysis should proceed on a section by section basis. *See, e.g.*, *Morrison*, 561 U.S. at 263–65 (holding that Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b), does not apply extraterritorially, but that Section 30(a), 15 U.S.C. § 78dd(a), does); *RJR Nabisco*, 136 S. Ct. at 2100-11 (holding that RICO's substantive provisions, 18 U.S.C. § 1962, apply extraterritorially to the extent the charged predicates apply extraterritorially, but that RICO's civil damages provision, 18 U.S.C. § 1964(c), does not). Accordingly, the focus of section 2703 alone – which is all about "[r]equired disclosure of customer communications or records" – is apparent not just from its title, but also from the fact that in each subsection, the exact same requirement – i.e., to disclose – applies without regard to the type of process that must issue as a precondition to the requirement. *See* 18 U.S.C. §§ 2703(b) (creating the same authority to require disclosure pursuant to warrants, subpoenas, and court orders under Section 2703(d)); *see also* 2703(c) (requiring disclosure pursuant to warrants, subpoenas, court orders, consent, and certain

written requests). Regardless of the process to be followed, the showing that must be made, or the level of information that must be disclosed, once the statute's requirements are met, the end result is that the provider is compelled to disclose the information described.[6] It is difficult to conceive of a section whose focus on disclosure could be clearer.

That is not to say there are no privacy concerns triggered by such disclosures, but the *Microsoft* court incorrectly concluded that those concerns trump the actual focus of Section 2703. Section 2703 *does* address privacy, by detailing when, and on what basis, the government can require the disclosure of certain information. The various processes and showings required reflect the way Congress balanced privacy concerns against the government's legitimate law enforcement needs. That, however, does not alter the language of the provision, which is about disclosure. *See Microsoft*, 829 F.3d at 218 (incorrectly surmising that had the Stored Communications Act "instead created . . . a rebuttable presumption of law enforcement access to content premised on a minimal showing of legitimate interest, the government's argument that the Act's focus is on aiding law enforcement and disclosure would be stronger."). There is nothing incongruous about conditioning disclosure obligations on certain processes, but requiring those processes to be followed in order to compel the disclosure does not change the simple conclusion that such processes are the procedural means to the substantive end: disclosure.

---

[6] *See* 18 U.S.C. § 2703(a) (requiring a warrant for disclosure "by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less"); § 2703(b) (setting rules for disclosure of specified information by a provider of remote computing service and requiring either a warrant, court order, or subpoena, depending on whether notice is provided to the subscriber); § 2703(c)(1) (applicable to disclosures of a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) and requiring either a warrant, court order, consent of the subscriber, or a formal request by law enforcement in certain enumerated circumstances); and § 2703(c)(2) (permitting a subpoena to require the disclosure specified basic subscriber information).

By looking at the other sections of the Stored Communications Act – Sections 2701 and 2702 – instead of only Section 2703, the Second Circuit came to the erroneous conclusion that Section 2703 was "an exception to" those other "primary" sections. That is a plain misapplication of the purpose of the section by section analysis because, as *RJR Nabisco* makes clear, different subsections of a statute can operate differently. 136 S. Ct. at 2102-03 (noting that the presumption of extraterritoriality may differ by subsection and it is only after performing the step one analysis on that basis is it appropriate to inquire into "focus"). The *Microsoft* court's error in this regard is all the more inexplicable, given that it appeared to otherwise acknowledge that, at the second step, it was required to look only to the territorial events that are the focus of "*the relevant statutory provision*." *Microsoft*, 829 F.3d at 216 (emphasis added).

The court then compounded that error when it concluded that requiring an entity in the United States to disclose information stored abroad results in an extraterritorial application of the statute. *See* pp. 5-8, *supra*. To the contrary, the law is clear that such compulsion occurs in the United States, on United States persons, and in United States courts.[7] Disclosure in accordance with the section's requirements is therefore, *not* an extraterritorial application of the statute. *See RJR Nabisco*, 136 S. Ct. at 2101 ("If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application *even if other conduct occurred abroad*.") (emphasis added). In exactly the same way as occurs for other types of compelled production of materials, *Hay Group*, 360 F.3d at 412, the compulsion to require the disclosure of information pursuant to process under the Stored Communications Act – whether the process that gives rise to the requirement is a subpoena, a court order under Section 2703(d), or a

[7] Indeed, such compulsion occurs only after a warrant is issued based on an application made to a court of competent jurisdiction in the United States.

warrant – occurs in the United States, and thus is not an extraterritorial application of Section 2703.[8] Indeed, as further discussed below in Subsection F, here, Google can *only* collect foreign-stored data responsive to a search warrant using their employees sitting in the United States.

Given that the entire purpose of the second step "focus" inquiry is to determine whether the subsection in dispute has sufficient domestic contacts to be considered a domestic application of law, thus avoiding extraterritorial concerns, the *Microsoft* court placed insufficient weight on these fundamental concepts and, instead, concluded "that the invasion of the customer's privacy takes place . . . where the customer's protected content is accessed – here, where it is seized by Microsoft, acting as an agent of the government." *Id.* at 216-20. Under the great weight of authority, however, any "invasion of the customer's privacy" occurs when the information is disclosed to the government in the United States and then searched pursuant to the warrant by investigators in the United States. As outlined in the attached warrant application, Google is not being asked to conduct a search of the information for evidence of the specified federal offenses. *Compare* Warrant Attachment B.I (describing the materials Google is required to disclose), *with* Warrant Attachment B.II (describing the information the government may search for and seize). Rather, the search of the disclosed information is conducted by the government in the United States. This two-step approach – first the disclosure of information by a provider, and second, its search by law enforcement – reflects the fact that Google is simply a custodian of certain information the court has determined should ultimately be searched by law enforcement for

[8] For that reason, the *Microsoft* court's concerns that "Microsoft will necessarily interact with the Dublin datacenter," 829 F.3d at 220, were misplaced. Nothing in the record showed "the citizenship and location of the customer," *id.* at 220, or for that matter, that the subscriber either had any right to prevent Microsoft from moving data anywhere it saw fit, or any knowledge about where the information resided. In fact, the notion that, in the Internet era, data resides in any particular geographic location is otherwise in considerable tension with the court's recognition that data today is properly thought of as "stored on the 'cloud'". *Id.*

evidence of crime. *See In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157 (D.D.C. 2014) (approving of the two-step approach to e-mail search warrants because "[e]nlisting a service provider to execute the search warrant could also present nettlesome problems"); *In the Matter of a Warrant for All Content & Other Info. Associated with the E-mail Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386, 395 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) (approving of two-step process in part because "[p]lacing the responsibility for performing these searches on the e-mail host would also put the host's employees in the position of appearing to act as agents of the Government vis-à-vis their customers"). In fact, Google has expressed a preference for this procedure. *In re Search of Google E-mail Accounts*, 99 F.Supp. 3d 992 (D. Alaska 2015) (sustaining Google's objection that it be required under a warrant to search for "communications with a minor, a person purporting to be or have access to a minor or which otherwise related to the 'enticement of a minor to engage in sexual activity for which any person can be charged with a criminal offense'" on the grounds that it was not competent to do).

The role of the provider in disclosing the information to be searched is precisely like the role of any party compelled to produce information. Contrary to the *Microsoft* court's assertion, persons compelled to testify or produce documents are not deemed to be agents of the government simply because they comply with their obligations ordered by a court or subpoena. *See, e.g., United States v. Miller*, 425 U.S. 435, 443-44 (1976) (finding that bank responding to subpoena for bank records is not an agent for the government, and applying the "general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time . . . the subpoena is issued"); *United States v. Bausch & Lomb Optical Co.*, 321 U.S. 707, 727 ("[T]he Fourth Amendment was

not intended to interfere with the 'power of courts to compel, through a subpoena duces tecum, the production, upon a trial in court, of documentary evidence,' so long as the scope of the subpoena was reasonable") (citations omitted); *Pentz v. United States*, 2011 WL 3269460, at *3 (M.D. Fla. July 29, 2011) (holding that a court-appointed Receiver in a civil responding to a subpoena issued in a criminal investigation was "acting as a private person" and "not acting as a government agent").

Finally, and importantly, the Second Circuit's application of the presumption against extraterritoriality is inconsistent with the very interest that the presumption is meant to serve. As stated by the Supreme Court, the "presumption [against extraterritoriality] 'serves to protect against unintended clashes between our laws and those of other nations which could result in international discord.'" *Kiobel*, 1333 S. Ct. at 1664 (citing *EEOC v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991)). As noted above, the Cybercrime Treaty is an agreement among the United States and 48 other countries "to adopt such legislative and other measures as may be necessary to empower its competent authorities to order . . . a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium." Cybercrime Treaty, Art. 18.1.a. As emphasized above, this provision focuses its territorial limit on the location of the person being ordered, not on the location of the system or storage medium, and the Explanatory Report explicitly recognizes that this power to compel disclosure extends to materials in the person's control.[9] Thus, a reading of the Stored Communications Act that permits courts to require disclosure by United States

[9] The recency of the Cybercrime Treaty and the resulting view that the Stored Communications Act need not be amended in order for the United States to fulfill its obligations under it mitigates the *Microsoft* court's concern that the Act was passed "almost thirty years ago" and that the "technological context" was very different back then. *Microsoft*, 829 F.3d at 205-06.

providers regardless of from where such information must be gathered will not "result in international discord[.]"

F. Application of The *Microsoft* Decision Here, Absurdly, Prevents the Government From Ever Requiring Google to Disclose Its Foreign-Stored Data

If, as Google requests, the *Microsoft* decision was adopted in this Circuit, then access to Google's foreign-stored data could *never* be compelled by the government: not pursuant to a lawful search warrant; not pursuant to valid international process; not otherwise. This preposterous result is, of course, not what Congress intended, and underscores the reasons why the *Microsoft* decision was incorrectly decided, and should not be applied here.

Google's network architecture automatically moves some of its users' data – including e-mails that contain attachments, and the attachments themselves – all around the world, at various times, depending upon the workings of an automatic computer algorithm aimed at creating network efficiency. Accordingly, the facts here are different than those in *Microsoft*.

In *Microsoft*, the computer systems used by Microsoft resulted in the data at issue being stored in a known datacenter in Ireland. Thus, Microsoft was able to tell the government specifically *where* the data was stored – in Ireland – and that *it would remain in Ireland* while the government sought legal process. Accordingly, once the government knew the location of the data stored abroad, the government could then proceed to obtain the data either under a Mutual Legal Assistance Treaty ("MLAT") request – if the United States had such a treaty with the country in which the data were stored – or, by using Letters Rogatory, a more cumbersome process. Thus, in a situation like that in *Microsoft*, the government could – theoretically, and through a much slower process – seek valid legal process to access Microsoft's data stored in Ireland.

Here, unlike in *Microsoft*, and for reasons explained below, the government will *never* be able to use valid legal process to compel access Google's user data stored abroad. Indeed, Google's

network architecture results in Google sending (and thus storing) Google user data – including e-mails containing attachments, and the attachments themselves – all over the world, at various times. The data, however, is a moving target: stored one day in a data center in Finland or Singapore; and automatically moved the next day to a new data center in Chile, or Belgium.[10] Further complicating things is that Google user data – such as an e-mail, or an e-mail attachment – is not stored as one single, cohesive digital file; instead, Google stores individual data files in multiple data "shards," each separate shard being stored in separate locations around the world. And, Google cannot even determine where its separate data shards are stored around the world at any given time; and, even if one shard were to stay in one place, without *all* of the shards being collected and put together at once to form the actual digital file, each shard alone is a useless piece of coded gibberish. Of course, each shard might move instantaneously to somewhere else; and then to somewhere else; and so on, and so forth.

What all this means, in lay terms, is that Google does not store its data abroad as one complete data file, on one specific server, for a specific period of time, located in one specific foreign country. Thus, the end result is that that Google's network architecture makes it *impossible* for the government to *ever* obtain Google's data stored abroad pursuant to *any* kind of legal process, including via MLAT request or Letters Rogatory. Seeking process through foreign nations takes time; it is no surprise that MLATs and Letters Rogatory take months, or even years, to fulfill. And therein lies the problem, and the critical distinction between the facts here and in *Microsoft*: in *Microsoft*, at least Microsoft could tell the government where it could seek to effect valid legal

[10] Google's website indicates that it "own[s] and operate[s] data centers around the world" in locations including: Taiwan, Chile, Singapore, Ireland, the Netherlands, Finland, and Belgium. *See* https://www.google.com/about/datacenters/inside/locations/index.html (last visited December 15, 2016). The United States does not have MLATs in place with all of these countries.

process, and that the data would remain in Ireland during that time period. The government could thus go get it, albeit slowly. In the present case, however, Google cannot tell the government where its user data is stored in various shards at any specific time, anywhere in the world. And even if Google could, by the time Google tells the government, Google's system could have moved the data multiple times.

Thus Google has created a system in which Google can retrieve the data, and its users can retrieve the data, but the government will only be able to obtain data that happens to be stored in the United States at the very moment when Google gathers the responsive information. Google cannot say where its foreign-stored data is today, and to the extent that it can, such data may be automatically moved to another server in another country within short periods. The government, therefore, cannot request the assistance of a foreign country using an MLAT request or Letters Rogatory, because no one knows which country to ask, and even if specific servers could be identified, the data may no longer be there by the time its location has been identified. Moreover, there are no Google employees in other countries that can access their foreign-stored data; instead, such data must, as a consequence of their network architecture, be accessed from a Google employee within the United States. And, thus, certain Google user data – even data that the government knows about, and writes about within a search warrant affidavit – is never accessible through compulsory legal process. Never.

Practically speaking, the absurd consequences of applying *Microsoft* here – wrong as that case is on the law – would mean that in any criminal investigation, be it national security, terrorism, child pornography, or human trafficking, where a suspected criminal located in the U.S. sends a Google e-mail containing an attachment to another suspected criminal also located in the U.S., Google's system automatically sends and stores that data abroad, in various shards, in various countries, at various times. And thus, for example, where a U.S. citizen in Chicago sends a Google e-mail with

an attachment containing evidence of crimes – say, instructions on how to infiltrate a U.S. nuclear power plant – to another U.S. citizen in Kansas City, while those e-mails and attachments could be accessed instantly by the sender and recipient on their computers – and by Google – at any time, the United States government would *never* be able to compel the disclosure of these e-mails – even where the government knows about the existence of such e-mails, obtains a lawful search warrant to obtain those e-mails, and those e-mails were not deleted by the sender and/or recipient, and thus still exist, fully accessible to the sender and recipient. This result, axiomatically, is not what Congress intended – and proves the serious flaws with the *Microsoft* decision.

Accordingly, the Second Circuit's reading of the Stored Communications Act, as it applies to this case and the thousands of future investigations that will be implicated, violates the basic principle of statutory construction that that a court should avoid a statutory interpretation that leads to absurd results. *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982); *In re Kaiser Aluminum Corp.*, 456 F.3d 328, 330 (3d Cir. 2006). If, as Google urges, this Court were to adopt the Second Circuit's incorrect reading of the statute in the *Microsoft* decision, any e-mail and cloud service provider can make itself immune from process by moving the data offshore and randomly moving it from country to country. Thus, a company could set up its headquarters in the United States to take advantage of an educated workforce, economic and social stability, and the rule of law, but become an "offshore bank" or "dark web" of data for criminals who are seeking to conceal their criminal conduct. Congress certainly cannot have intended such an absurd result when it passed Section 2703.[11]

---

[11] Professor Orin Kerr recently commented on the absurdity of these results in the Volokh Conspiracy blog in the Washington Post. Kerr, The Surprising Implications of the Microsoft/Ireland Warrant Case, November 29, 2016. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/?utm_term=.53287b65cf5d.

G. This Court Should Not Limit its Ruling to the Facts Related to a Provider's Network Architecture.

As set forth above in Section F, application of the *Microsoft* decision in light of Google's network architecture leads to the absurd result that the government cannot, using any type of legal process, compel the production of foreign-stored information. However, the government seeks a ruling based on the law as opposed to the specific facts of Google's network architecture. Otherwise, application of the *Microsoft* ruling would require governmental and judicial inquiry into every different type of architecture that providers of services, such as Google, use to store data, which may include inquiry into proprietary information of the provider. Such an inquiry would require the provider to disclose in what country the data is stored,[12] how long it will be stored there, how frequently it is moved, and whether it has employees in that country who can access the data to comply with an international request from the United States, using the procedures of a mutual legal assistance treaty or Letters Rogatory. This also means that anytime a provider implements changes in its architecture, a new inquiry may be required.

Additionally, a fact-specific ruling that does not directly engage the Second Circuit's reasoning in the *Microsoft* decision would create perverse incentives for providers. As manifested by the distinctions between how Microsoft handled its data at the time of the *Microsoft* decision and how Google handles its data now, providers have differing methods for storing data across large global networks as a result of their own business decisions. A fact-

[12] Indeed, as apparent from Google's response, such an inquiry could prove rather difficult in light of its apparent inability to identify the geographic location of some of the records called for in the search warrant at issue. *See* Google's Response at 5 ("The warrant also cannot reach records if it is unknown whether the records are located in the United States.").

specific application of the *Microsoft* decision would put another consideration into providers' otherwise purely business choice. A provider wishing to cooperate in every way with U.S. law enforcement would be discouraged from using a cloud-based architecture utilizing servers in foreign facilities. Instead, such companies would be incentivized to store all data for a particular user account in one server, domestically or overseas, whether or not such a network architecture is the best and most efficient way to handle the data and to make it available to that company's users. However, because the *Microsoft* court was simply incorrect to conclude that the Stored Communications Act does not reach a U.S. provider's foreign-stored data,[13] there is no good reason for this Court to limit its ruling to the facts of Google's network architecture and to create such incentives.

II. THE NON-DISCLOSURE ORDER

Because process to Internet Service Providers frequently is sought early in an investigation, when the scope and the length of the investigation cannot be determined, the government frequently, as it did in this case, requests an open-ended non-disclosure order under 18 U.S.C. § 2705(b). The statute does not prohibit them. It permits the court to enter a non-disclosure order "for such period as the court deems appropriate," 18 U.S.C. § 2705(b). Google objects on First Amendment grounds that the order is a prior restraint on its speech.

Google's position is overstated. In criminal investigations, whether grand jury or otherwise, the balance is struck in favor of secrecy. Google fails to cite any Third Circuit precedent to support its position, and the government is aware of none. Third Circuit law, as well as the law in other circuits, is to the contrary. In *First Amendment Coalition v. Judicial Inquiry and Review*

[13] For the same reason, the notion that Congress could address the issues created by the *Microsoft* decision is inapposite. *See* Google's Response at 6. The statute is not the problem; the *Microsoft* decision's interpretation of the statute is the issue before this Court.

Board, 784 F.2d 467 (3d Cir. 1986) (hereafter "*JIRB*"), the court upheld the secrecy requirements of investigations of the Board. It only struck down a bar on witnesses reporting their own testimony. The court held that a witness before the JIRB could report on his own testimony. It could also report on facts about the investigation, if it had obtained them from an independent source. The witness could not report on matters that it had learned from participating in the proceeding.[14] (A witness' testimony before the proceeding would necessarily be about facts that s/he learned independent of the proceeding. There would be no need for the Board to call the witness otherwise.) The Court stated:

> It follows that although witnesses may, if they choose, disclose their own testimony, they may not reveal that of another witness whom they may hear testify. Nor are they free to disclose the comments of Board members or staff that are overheard during their appearance.

JIRB, 784 F.2d at 479.

In so ruling, the court followed the Supreme Court's ruling in *Seattle Times v. Rhinehart*, 467 U.S. 20 (1984), in which the Supreme Court upheld a bar on a newspaper's publication of facts that it had learned through the court's discovery process while it was a party to the litigation. *See also Kamasinski v. Judicial Review Council*, 44 F.3d 106 (2d Cir. 1994). The Court in *JIRB* noted that the Supreme Court had distinguished between facts that a newspaper learned as a result of its own investigation, *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978), and those which it learned as a participant in the legal process. *Seattle Times*. In *JIRB*, the court held that a witness could reveal his or her own testimony, but no more. Google's only testimony in this matter would be its act of production. It certainly does not propose to reveal the contents that it has turned over, or will turn over. That is information that it knows independent of the legal

[14] *See also Stilp v. Contino*, 613 F.3d 405 (3d Cir. 2010).

proceeding. [15] Instead, it proposes to disclose the existence of the warrant; a fact it knows only because of the legal process.

In the context of criminal investigations, the concern for secrecy is even greater. This case involves both grand jury and non-grand jury aspects. In that context, the law is similar to what the Third Circuit has expounded for the judicial review board. *Hoffman-Pugh v. Keenan*, 338 F.3d 1136, 1140 (10th Cir. 2003); *In re Subpoena to Testify before Grand Jury*, 864 F.2d 1559, 1564 (11th Cir. 1989).

Of course, once a grand jury investigation has ended, a restriction on disclosure of one's own testimony is improper. *Butterworth v. Smith*, 494 U.S. 624 (1990). Here, however, the investigation is not over. The act of disclosure could still result in the destruction of evidence.

Google only knows of the search warrant because it has been served. It knows no facts about this matter other than what is has learned from service of the search warrant. Thus, under existing Third Circuit precedent, this Court's ban on disclosure was proper.

As of this date, the target is not aware of the government's investigation. There is a serious risk that if the target should learn about the government's investigation, he may destroy evidence or otherwise attempt to obstruct this investigation. Moreover, disclosure of the existence of this search warrant could also jeopardize other investigation actions the government is currently undertaking against the target.

---

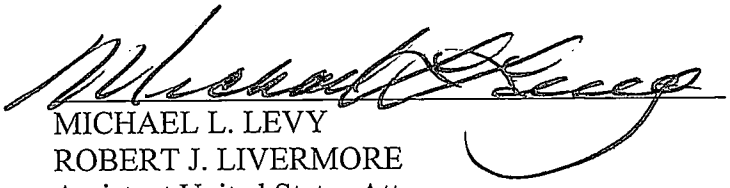
[15] Title 18, United States Code, Section 2702 prohibits Google from disclosing the contents of a holder's account, unless one of the statutory exceptions applies.

IV. CONCLUSION

For the reasons set forth above, the government respectfully requests the Court to enforce the search warrant and to direct Google, Inc., to produce the contents of the account, no matter where in the world they may be stored.

Respectfully submitted,

LOUIS D. LAPPEN
Acting United States Attorney



MICHAEL L. LEVY
ROBERT J. LIVERMORE
Assistant United States Attorneys

ANDREW S. PAK
Trial Attorney
Computer Crime & Intellectual Property Section
United States Department of Justice

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing motion was served via e-mail upon the following counsel for Google:

Todd M. Hinnen, Esq.
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
THinnen@perkinscoie.com

John (Randy) R. Tyler, Esq.
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
RTyler@perkinscoie.com

William A. DeStefano
Stevens & Lee
818 Market Street, 29th Floor
Philadelphia, PA 19103
wad@stevenslee.com

MICHAEL L. LEVY
Assistant United States Attorney

Date: January 4, 2017